

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 2 of 19

Attorney's Docket No.: 10664-147001

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A computer-implemented method, ~~for transmitting a message from a sender to an intended recipient~~ comprising:
 - encrypting a message using a symmetric key to generate an encrypted message;
 - sending the encrypted message to an intended recipient without making the symmetric key immediately accessible to the intended recipient;
 - providing the symmetric key to a third party; and
 - if the intended recipient signs and returns to the third party a receipt including a representation of the encrypted message, transferring, by the third party, the receipt to a sender and providing the symmetric key to the intended recipient.
2. (Currently Amended) The computer-implemented method of claim 1 wherein the receipt signed by the intended recipient contains an identifier computed from the message and the symmetric key using a cryptographically secure hash functions function.
3. (Currently Amended) A computer-implemented method, ~~for transmitting a message from a sender to an intended recipient~~ comprising:
 - at a sender, encrypting a message using a symmetric key, encrypting the symmetric key to make the symmetric key accessible to a third party but not immediately accessible to an intended recipient and sending the encrypted message and the encrypted symmetric key to the intended recipient;
 - at the intended recipient, signing a receipt including a representation of the encrypted message and sending the receipt and the encrypted symmetric key to the third party; and

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 3 of 19

Attorney's Docket No.: 10664-147001

at the third party, transferring the receipt to the sender and providing the symmetric key to the intended recipient if the receipt is properly signed.

4. (Currently Amended) A computer-implemented method for certifying receipt of a message, the message being sent from a sender to an intended recipient and being encrypted by a symmetric key, and the method executing at a third party distinct from the sender and the intended recipient, the method comprising:

receiving a signed receipt and an encrypted symmetric key from an intended recipient, the signed receipt memorializing receipt of the encrypted message by the intended recipient;
verifying the signed receipt;
transferring the verified receipt to a sender; and
providing the symmetric key to the intended recipient.

5. (Currently Amended) A computer-implemented method for certifying receipt of a message, the message being sent from a sender to an intended recipient and being encrypted by a symmetric key, the method executing at a third party distinct from the sender and the intended recipient, the method comprising:

receiving a separately encrypted message header associated with ~~the a~~ message and a certified receipt originating from an intended recipient, the certified receipt including a first message identifier signed by the intended recipient;

decrypting the separately encrypted message header to expose a symmetric key and the a second message identifier;

verifying the certified receipt, including verifying ~~the a~~ signature of the intended recipient and ~~that the first and second message identifiers are the equivalent in the certified receipt is the same as the message identifier obtained from the separately encrypted message header~~; and

after verifying the certified receipt, forwarding the certified receipt to the sender; and forwarding the symmetric key to the intended recipient.

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 4 of 19

Attorney's Docket No.: 10664-147001

6. (Currently Amended) A computer-implemented method, for transmitting a message from a sender to an intended recipient comprising:

encrypting a message using a symmetric key;
~~storing the symmetric key and the message;~~
sending the encrypted message to an intended recipient without the symmetric key;
forwarding the encrypted symmetric key to a third party; and
receiving from the third party a certified receipt verified by the third party indicating receipt of the message by the intended recipient.

7. (Currently Amended) A computer-implemented method, for transmitting a message from a sender to an intended recipient comprising:

~~identifying a message for transmission to an intended recipient;~~
creating a message header that includes a symmetric key and a message identifier associated with the ~~a message for transmission to an intended recipient~~;
encrypting the message using the symmetric key;
public key encrypting the message header using a public key of a third party;
attaching the message header to the encrypted message forming a certified message and forwarding the certified message to the intended recipient;
~~storing a copy of the certified message and the symmetric key;~~
receiving a certified receipt originating from ~~an~~ the intended recipient, the certified receipt being verified at the third party and forwarded to the ~~a~~ sender after verification; and
verifying validity of the receipt using the stored symmetric key and the certified message.

8. (Currently Amended) A computer-implemented method for providing a receipt for a message, the message being sent from a sender to an intended recipient and the method executing at the recipient, the method comprising:

receiving an encrypted message from a sender, the encrypted message encrypted by a symmetric key;

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 5 of 19

Attorney's Docket No.: 10664-147001

creating a signed receipt for the encrypted message including signing a hash of the encrypted message and returning the signed receipt to a third party;

after verification of the signed receipt at the third party, receiving the symmetric key from the third party; and

decrypting the encrypted message using the symmetric key.

9. (Previously Presented) The computer-implemented method of claim 8 wherein the step of receiving the symmetric key includes not receiving the symmetric key until a successful transfer of the signed receipt to the sender.

10. (Currently Amended) The computer-implemented method of claim 6, further comprising:

storing a copy of the certified receipt and the symmetric key; and

verifying the validity of the certified receipt using the stored symmetric key and the certified message.

11. (Currently Amended) A computer-implemented method for generating a receipt associated with a message, where the receipt is created without exposing the content of the message to an intended recipient, comprising:

receiving a message encrypted by a symmetric key;

receiving a hash of the symmetric key; and

generating a receipt including generating a message identifier prior to decrypting the message, the message identifier including a representation of the hash of the symmetric key and the message encrypted by the symmetric key[;],

wherein the message identifier is able to be used to verify receipt of the message at the intended recipient without exposing the message content to an intended recipient.

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 6 of 19

Attorney's Docket No.: 10664-147001

12. (Currently Amended) The computer-implemented method of claim 11, wherein:
generating a receipt including a message identifier includes using a hash function to
generate the message identifier.

13. (Previously Presented) The computer-implemented method of claim 11, further
comprising:

receiving a first message identifier at the intended recipient;
the generating step including generating a receipt including a second message identifier,
at the intended recipient; and
sending the receipt and the first message identifier to a third party.

14. (Currently Amended) The computer-implemented method of claim 13, further
comprising:

receiving the receipt, at the third party;
verifying the receipt without accessing the message content; and
providing the receipt to a sender.

15. (Currently Amended) The computer-implemented method of claim 11, where:
the message is encrypted with the symmetric key prior to sending to the intended
recipient; and

the symmetric key is sent to the intended recipient from a third party so that the intended
recipient can decrypt the message.

16. (Previously Presented) The computer-implemented method of claim 11, further
comprising:

sending the encrypted symmetric key to the intended recipient with the message;
at the intended recipient, sending the encrypted symmetric key to a third party with a
receipt that includes a representation of the message identifier; and

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 7 of 19

Attorney's Docket No.: 10664-147001

sending the receipt to a sender after verification of the receipt.

17. (Currently Amended) A computer-implemented method for generating a signed receipt associated with a message without exposing the content of the message, comprising:
 - receiving a message encrypted by a symmetric key;
 - receiving a hash of the symmetric key;
 - generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key; and
 - signing the representation to generate a signed receipt[[;]].wherein the signed receipt is generated prior to decrypting the message and receiving the symmetric key.
18. (Currently Amended) The computer-implemented method of claim 17, further comprising:
 - sending the signed receipt to a third party for transfer to a sender; and
 - verifying the validity of the signed receipt at the third party.
19. (Currently Amended) The computer-implemented method of claim 18, further comprising:
 - allowing a recipient access to the content of the message if the signed receipt is verified at the third party.
20. (Canceled)
21. (Canceled)

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 8 of 19

Attorney's Docket No.: 10664-147001

22. (Currently Amended) A computer-implemented method for time-stamping a message without exposing the content of the message to a time stamping authority, comprising:

encrypting the a message using a symmetric key;

computing a hash of the symmetric key;

generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key; and

time-stamping the representation, including sending the representation to a time-stamping authority and receiving from the time-stamping authority a time stamp certificate including the representation, a time, and a sender identification and a recipient identification for the message.

23. (Currently Amended) A computer-implemented method for time-stamping a message without exposing the content of the message to a time stamping authority, comprising:

encrypting the a message using a symmetric key;

computing a hash of the symmetric key;

generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key; and[[:]]

time-stamping the representation, including sending the representation to a time-stamping authority and receiving from the time-stamping authority a time stamp certificate including the representation, a time, a sender identification and a recipient identification for the message and at least one of a public key of the sender and a public key of the recipient.

24. (Currently Amended) A computer-implemented method for generating a signed receipt certifying that a message has been received at a particular time by an intended recipient, without exposing the message content of the message, comprising:

receiving a message having content, wherein the message is encrypted by a symmetric key;

receiving a hash of the symmetric key;

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 9 of 19

Attorney's Docket No.: 10664-147001

generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key, wherein the representation is generated prior to decrypting the message and receiving the symmetric key; and

time-stamping the representation, including sending a time stamp certificate including the representation, a time, and a sender identification and a recipient identification for the message; and

signing the time-stamped representation.

25. (Currently Amended) The computer-implemented method of claim 24, further comprising:

sending the time-stamped representation to a third party such that the time stamp can be verified by the third party without exposing the content of the message to the third party; and
verifying the validity of the signed receipt at the third party.

26. (Currently Amended) The computer-implemented method of claim 25, further comprising:

allowing an intended recipient access to the content of the message if the signed receipt is verified at the third party.

27. (Currently Amended) A computer-implemented method for generating a signed receipt for a message certifying a sending time and a receiving time by an intended recipient without exposing the content of the message, comprising:

receiving a message encrypted with a symmetric key;
receiving a hash of the symmetric key;
receiving a time-stamped a time stamp certificate including a representation of the hash of the symmetric key and the encrypted message, a time, and a sender identification and a recipient identification for the message, the time stamp certificate, the representation being time-stamped at time of sending;

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 10 of 19

Attorney's Docket No.: 10664-147001

time-stamping the representation at a time of receiving;
combining the representation time-stamped at the time of sending and the representation time-stamped at the time of receiving providing to provide a combined receipt; and
signing the combined receipt; and
sending the combined receipt to a third party such that the combined receipt can be verified by the third party without exposing the content of the message to the third party.

28. (Currently Amended) The computer-implemented method of claim 27, further comprising:

verifying the validity of the signed receipt at the third party.

29. (Currently Amended) The computer-implemented method of claim 27, further comprising:

allowing an intended recipient access to the content of the message if the signed receipt is verified at the third party.

30. (Previously Presented) The computer-implemented method of claim 1, further comprising:

computing a hash of the symmetric key; and

making the hash of the symmetric key accessible to the intended recipient, wherein the receipt contains a representation of the symmetric key.

31. (Currently Amended) A computer-implemented method for securing securely sending a message, comprising:

encrypting a message using a symmetric key;

computing a hash of the symmetric key; and

generating a representation of the hash of the symmetric key and the encrypted message; encrypted by the symmetric key.

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 11 of 19

Attorney's Docket No.: 10664-147001

sending a request including the representation to a time stamping authority;
receiving from the time stamping authority a time stamp certificate including a time
stamped representation of the hash of the symmetric key and the message encrypted by the
symmetric key;
generating a certified message including the time stamp certificate; and
sending the certified message to a recipient.

32. (Previously Presented) The computer-implemented method of claim 31, wherein:
generating the representation includes using a one-way hash.

33.-35. (Canceled)

36. (Currently Amended) A computer-implemented method of for securely sending and receiving a message, using a third party to verify the authenticity of the message, comprising:
at a sender:

encrypting a message using a symmetric key to generate an encrypted message;
sending the encrypted message to an intended recipient without making the symmetric key immediately accessible to the intended recipient; and
providing the symmetric key to a third party;

at the intended recipient:

receiving the encrypted message from the sender;
creating a signed receipt for the encrypted message, including signing a hash of the encrypted message and returning the signed receipt to the third party;

after verification of the signed receipt at the third party, receiving the symmetric key from the third party; and

decrypting the encrypted message using the symmetric key;
at the third party:

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 12 of 19

Attorney's Docket No.: 10664-147001

receiving the signed receipt from the recipient;
verifying the signed receipt;
transferring the verified receipt to the sender; and
providing the symmetric key to the intended recipient.

37. (Currently Amended) The computer implemented method of claim 36, wherein:

at the sender:

sending the encrypted message to ~~an~~ the intended recipient includes encrypting the symmetric key with a public key of the third party and sending the encrypted symmetric key to the intended recipient so that the intended recipient cannot access the symmetric key or the message prior to the intended recipient returning the signed receipt to the third party; and

encrypting a the message using a symmetric key to generate ~~an~~ the encrypted message includes creating a first hash of encrypted content of the message and including the first hash of the encrypted content in the encrypted message;

at the intended recipient:

returning the signed receipt to the third party includes creating a second hash of the encrypted content in the message, sending the second hash of the encrypted content in the message, forwarding the encrypted symmetric key to the third party for the third party to decrypt the key, but not sending the encrypted content message to the third party;

at the third party:

providing the symmetric key to the intended recipient after verifying the signed receipt from the intended recipient;

verifying the signed receipt includes verifying that the first hash of the encrypted content equals the second hash of the encrypted content; and

providing the symmetric key to the intended recipient includes decrypting the encrypted symmetric key sent by the recipient.

38. (Currently Amended) The computer-implemented method of claim 1, wherein:

sending the encrypted message to ~~an~~ the intended recipient includes encrypting the

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 13 of 19

Attorney's Docket No.: 10664-147001

symmetric key with a public key of the third party and sending the encrypted symmetric key to the intended recipient so that the recipient cannot access the symmetric key or the message prior to the intended recipient returning the signed receipt to the third party; and

encrypting a message using a symmetric key to generate an encrypted message includes creating a first hash of encrypted content of the message and including the first hash of the encrypted content in the encrypted message.

39. (Previously Presented) The computer-implemented method of claim 3, further comprising:

at the sender, creating a first hash of encrypted content of the message and sending the first hash to the recipient;

at the recipient, creating a second hash of the encrypted content in the message, sending the second hash to the third party and decrypting the encrypted message after receiving the symmetric key from the third party; and

at the third party, comparing the first hash to the second hash to verify that the first hash is equal to the second hash, decrypting the encrypted symmetric key, wherein providing the symmetric key does not occur until after comparing the first and second hashes.

40. (Previously Presented) The computer-implemented method of claim 4, further comprising:

decrypting the encrypted symmetric key for providing to the intended recipient.

41. (Currently Amended) The computer-implemented method of claim 40, wherein:

decrypting the encrypted symmetric key includes decrypting the encrypted symmetric key received from the intended recipient, wherein the intended recipient received the encrypted symmetric key from the sender.

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 14 of 19

Attorney's Docket No.: 10664-147001

42. (Previously Presented) The computer-implemented method of claim 4, wherein: providing the symmetric key to the intended recipient occurs after verifying the signed receipt.

43. (Currently Amended) The computer-implemented method of claim 4, wherein: verifying the signed receipt includes determining that a hash of the encrypted message created by the sender is equivalent to a hash of the encrypted message created by the intended recipient.

44. (Previously Presented) The computer-implemented method of claim 4, wherein: verifying the signed receipt ensures that the intended recipient received an encrypted message sent by the sender.

45. (Previously Presented) The computer-implemented method of claim 5, wherein the message identifier includes a hash of the encrypted message, the method further comprising: verifying that the message identifier signed by the intended recipient equals the message identifier in the separately encrypted message header.

46. (Previously Presented) The computer-implemented method of claim 5, wherein: forwarding the symmetric key to the intended recipient occurs after verifying the certified receipt.

47. (Previously Presented) The computer-implemented method of claim 6, wherein: forwarding the encrypted symmetric key to the third party without exposing the message to the third party.

48. (Previously Presented) The computer-implemented method of claim 7, wherein the method does not include sending the message to the third party.

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 15 of 19

Attorney's Docket No.: 10664-147001

49. (Previously Presented) The computer-implemented method of claim 8, further comprising:

receiving a first hash of the encrypted message from the sender;
hashing the encrypted message to create a second hash of the encrypted message; and
sending the first and second hashes to the third party for the third party to verify that the first hash equals the second hash.

50. (Currently Amended) The computer-implemented method of claim 17, wherein further comprising:

receiving a first hash of encrypted content;
hashing the received encrypted message content to create a second hash of the encrypted content; and
sending the first and second hashes to a third party for verification.

51. (Currently Amended) The computer-implemented method of claim 31, further comprising:

sending the representation of the hash of the symmetric key and the encrypted message ~~encrypted by the symmetric key~~ to an intended recipient, wherein the intended recipient does not have access to the symmetric key for decrypting the encrypted message at the time of receipt ~~receiving the encrypted message~~.